

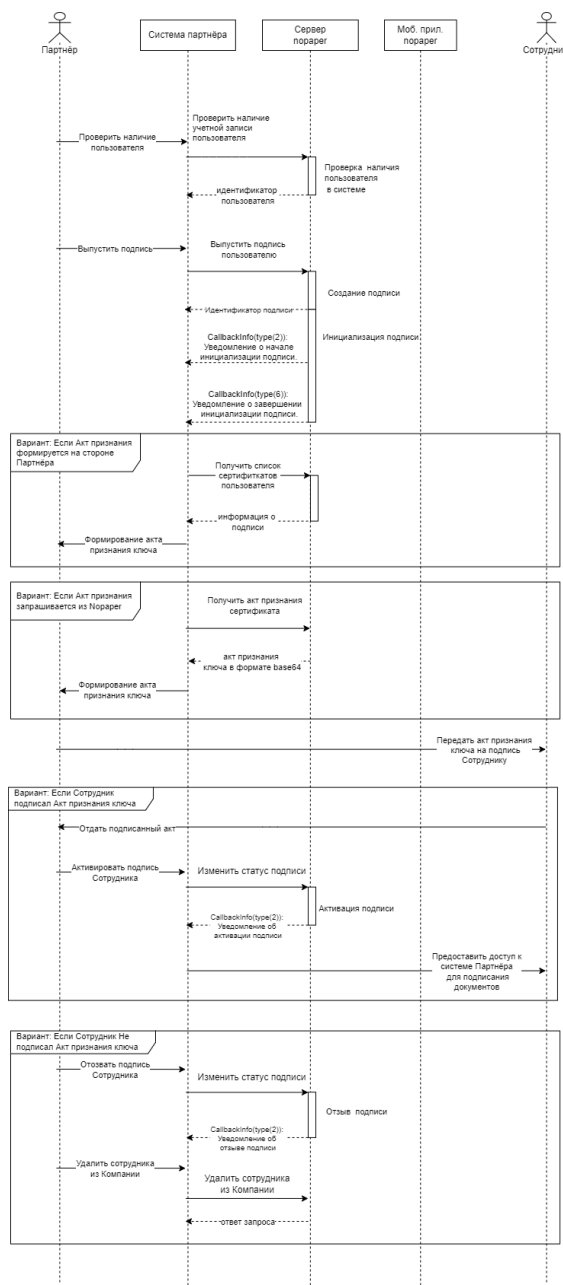
Сценарий выдачи Серверной подписи сотруднику через API Noparer

1. Диаграмма последовательности вызова методов REST-API	3
2. Общее описание выдачи серверной подписи через REST-API	4
2.1. Проверить наличие пользователя	4
2.2. Создать подпись сотруднику	4
2.3. Получить информацию о подписях Пользователя	5
2.4. Получить акт признания ключа сотрудника (опционально)	6
2.5. Активировать подпись сотрудника	7
2.6. Заблокировать/разблокировать подпись сотрудника	7
2.7. Отозвать подпись сотрудника	7
3. Описание REST-API noparer	8
3.1. Проверить наличие пользователя	8
1. Авторизация	8
2. Входные параметры	8
3. Выходные параметры	8
4. Таблица кодов ошибок	9
3.2. Создать подпись сотруднику	10
1. Авторизация	10
2. Входные параметры	10
3. Выходные параметры	11
4. Таблица кодов ошибок	12
3.3. Получить информацию о подписях сотрудника	12
1. Авторизация	13
2. Входные параметры	13
3. Выходные параметры	13
4. Таблица кодов ошибок	16
3.4. Получить акт признания ключа для сертификата	16
1. Авторизация	16
2. Входные параметры	16
3. Выходные параметры	17
4. Таблица кодов ошибок	18
3.5. Активировать подпись сотрудника	18

[postman collection](#) (версия 1.0)

1. Авторизация	18
2. Входные параметры	18
3. В синхронном режиме сервис вернёт статус выполнения запроса.	19
4. Таблица кодов ошибок	19
3.6. Заблокировать/активировать подпись	20
1. Авторизация	21
2. Входные параметры	21
3. Выходные параметры	21
4. Таблица кодов ошибок	22
3.7. Отозвать подпись сотрудника	23
1. Авторизация	23
2. Входные параметры	23
3. Выходные параметры	23
4. Таблица кодов ошибок	24

1. Диаграмма последовательности вызова методов REST-API



(открыть/скачать изображение можно нажав на него)

2. Общее описание выдачи серверной подписи через REST-API

2.1. Проверить наличие пользователя

Система партнёра может проверять наличие пользователя в порарер. Для этого необходимо выполнить запрос «Проверить наличие пользователя в порарер» `/partner-api/api/v2/external/profile-fl/user-guid/by-phone`. В запросе требуется передать номер телефона будущего пользователя. В ответе порарер вернёт `userGuid` действующего пользователя или сообщение, что пользователь не найден.

Примечания:

- Запрос принимает российский номер телефона в формате 79*****.

2.2. Создать подпись сотруднику

Система партнёра может создавать серверную подпись Сотрудникам своей компании в порарер. Серверная подпись позволяет подписывать документы от имени компании без использования мобильного приложения порарер.

Для этого необходимо выполнить запрос «Создать сертификат payControlServer» `/partner-api/api/v2/external/certificate/pay-control/pc-server`. В запросе требуется передать `userGuid` – идентификатор Пользователя, полученный из п.2.1., и `acceptanceType` – настройку, которая отвечает на чьей стороне будет сгенерирован акт признания ключа (документ подтверждающий принятие подписи):

- если настройка 1 – то акт признания ключа необходимо будет скачать из системы Норарер (п.2.4.),
- если настройка 2 – то акт признания ключа генерируется самостоятельно на стороне Партнёра на основании полученной информации о подписи ( Очная верификация ЮЛ.docx).

В ответе порарер вернёт `certificateId` – идентификатор подписи. `certificateId` необходимо сохранить в системе партнёра, чтобы использовать при вызове других методов API.

[postman collection](#) (версия 1.0)

Норпер создает подпись НЕ активной **providerStatus=3** (initialization). Для подписания документов подпись необходимо будет активировать (п.2.8).

Примечания:

- При изменении статуса подписи в статус Initialization система норпер отправит уведомление о изменении статуса подписи (см. диаграмму последовательности);
- После завершения инициализации подписи система норпер также отправит уведомление о завершении инициализации подписи (см. диаграмму последовательности), при этом подпись также останется в статусе **Initialization**.
- При изменении статуса сертификата, который создан Партнёром, отправляется **CallbackInfo(type(2))** (подробнее в документации [Работа с уведомлениями call-back API Nopaper](#) - п.4.2.)

2.3. Получить информацию о подписях Пользователя

Система партнёра может получать информацию подписях Пользователя в норпер. Для этого необходимо выполнить запрос «Получить список сертификатов Пользователя» **/partner-api/api/v2/external/certificate/list**. В запросе требуется передать **userGuid** — идентификатор пользователя, который получен при проверке наличия пользователя п.2.1. или при регистрации п.2.2. В ответе норпер вернёт список подписей Сотрудника (массив объектов) во всех статусах, с ключевой информацией о каждой подписи.

Список статусов подписи:

- **status=1** (Template) — шаблон подписи
- **status=2** (Initialization) — инициализация подписи
- **status=3** (initializationError) — ошибка при инициализации подписи
- **status=4** (Available) — подпись активна

[postman collection](#) (версия 1.0)

- **status=5** (Blocked) — подпись заблокирована
- **status=6** (Revoked) — подпись отозвана

Информация о подписи нужна чтобы сформировать и подписать с Сотрудником Акт признания ключа, которым Сотрудник признает использование выпущенной подписи.

Примечания:

- Норпер не может вернуть информацию о подписи в полном объёме в момент создания п.2.2, полная информация о подписи приходит после того как подпись завершит инициализацию подписи. Инициализация подписи в системе норпер происходит практически мгновенно после создания.
- Можно использовать этот метод API для синхронизации данных между системами в исключительных ситуациях;
- Партнёр может получить только информацию о подписях, которые сам создал/выдал. Если Клиент получил подпись самостоятельно в норпер, то подпись не вернётся партнёру в ответе на запрос.

2.4. Получить акт признания ключа сотрудника (опционально)

Система партнёра может получить акт признания ключа Сотрудника, которому выдала подпись. Для этого необходимо выполнить запрос «Получить акт признания ключа для сертификата»

/partner-api/api/v2/external/certificate/pay-control/{certificateId}/act-acceptance-key. В запросе требуется передать **certificateId** — идентификатор подписи, который получен при создании подписи п.2.2. В ответе норпер вернёт статус выполнения запроса.

Примечания:

- Норпер не может вернуть акт признания ключа в момент создания п.2.2, акт признания ключа можно получить только после того как подпись завершит инициализацию подписи. Инициализация подписи в системе норпер происходит практически мгновенно после создания.

2.5. Активировать подпись сотрудника

Система партнёра может активировать подпись Сотрудника своей компании в порAPER. Для этого необходимо выполнить запрос «Активировать сертификат Pay-control» `/partner-api/api/v2/external/certificate/pay-control/{certificateId}/activate`. В запросе требуется передать `certificateId` — идентификатор подписи, который получен при создании подписи п.2.2. В ответе порAPER вернёт статус выполнения запроса.

Примечания:

- Активировать акт признания ключа можно только после завершения инициализации подписи.

2.6. Заблокировать/разблокировать подпись сотрудника

Система партнёра может заблокировать/разблокировать подпись Сотрудника своей компании в порAPER, если необходимо заблокировать подпись с возможностью её дальнейшей активации. Для этого необходимо выполнить запрос «Заблокировать/разблокировать сертификат Pay-control» `/partner-api/api/v2/external/certificate/pay-control/{certificateId}/blocking-control`. В запросе требуется передать `certificateId` — идентификатор подписи, который получен при создании подписи п.2.2 и параметр `isBlock` отвечающий за блокировку/разблокировку подписи. В ответе порAPER вернёт статус выполнения запроса.

2.7. Отозвать подпись сотрудника

Система партнёра может отозвать подпись Сотрудника своей компании в порAPER, если необходимо заблокировать подпись без возможности её дальнейшей активации. Для этого необходимо выполнить запрос «Отозвать сертификат Pay-Control» `/partner-api/api/v2/external/certificate/pay-control/{certificateId}/revoke`. В запросе требуется передать `certificateId` — идентификатор подписи, который получен при создании подписи п.2.5. В ответе порAPER вернёт статус выполнения запроса.

3. Описание REST-API порарер

3.1. Проверить наличие пользователя

Вызов: GET запрос в порарер

Формат: JSON

/partner-api/api/v2/external/profile-fl/user-guid/by-phone

1. Авторизация

API Key

2. Входные параметры

Параметр	Тип	Обязательность	Описание	Расположение параметра
userPhone	string	Да	Номер телефона пользователя	Query

Пример запроса

```
https://np-demo.abanking.ru/partner-api/api/v2/external/profile-fl/user-guid/by-phone?userPhone=79505421870
```

3. Выходные параметры

В синхронном режиме сервис вернёт статус выполнения запроса.

Code	Description
200	Success
400	Error
401	Unauthorized
403	Forbidden

В случае успешного запроса сервис вернёт параметры:

Параметр	Тип	Описание
userGuid	string	Идентификатор пользователя

Пример ответа с кодом 200

```
{  
  "userGuid": "e1e0896f-8368-4c8b-afb4-daf7542dabd5"  
}
```

4. Таблица кодов ошибок

Код	Текст	Комментарий
NOPAPERPARTNERLIB.10401	profile by phone not found	Пользователь с данным номером телефона не найден в сервисе

[postman collection](#) (версия 1.0)

NOPAPERPARTNERAPI.CORE.41116	Request body was not converted to model	Переданная модель запроса не может быть обработана
------------------------------	---	--

Пример ответа с кодом 400

```
{
  "description": "profile by phone not found",
  "code": "NOPAPERPARTNERLIB.10401"
}
```

3.2. Создать подпись сотруднику

Вызов: **POST** запрос в **nopaper**Формат: **JSON****/partner-api/api/v2/external/certificate/pay-control/pc-server**

1. Авторизация

API-key

2. Входные параметры

Параметр	Обязательность	Тип	Описание	Расположение параметра
userGuid	Да	string	Идентификатор пользователя	Query

[postman collection](#) (версия 1.0)

acceptanceType	Да	Enum	Настройка – где будет генерироваться акта признания ключа <i>1 – в порарер;</i> <i>2 – на стороне Партнёра.</i>	Query
----------------	----	------	---	-------

Пример запроса

```
https://np-demo.abanking.ru/partner-api/api/v2/external/certificate/pay-control/pc-server?userGuid=aad2bb59-ee60-4965-9331-8c7f1d690ed3&responsiblePartyForAcceptanceAct=1
```

3. Выходные параметры

В синхронном режиме сервис вернёт статус выполнения запроса.

Code	Description
200	Success
400	Error
401	Unauthorized
403	Forbidden

В случае успешного запроса сервис вернёт параметры:

Параметр	Тип	Описание
----------	-----	----------

certificateId	string(\$uuid)	Идентификатор сертификата
---------------	----------------	---------------------------

Пример ответа 200

```
"certificateId": "cbac783c-629e-4133-ab32-de31e74d0154"
```

4. Таблица кодов ошибок

Код	Текст	Комментарий
NOPAPERPARTNER. 10300	Cannot be created certificate without fullname profile fl	У пользователя отсутствует имя или фамилия
NOPAPERPROFILEU L.01005	Employee not found by userGuid = {userGuid} and companyId = {companyId}	Пользователь не является сотрудником компании

Пример ответа с кодом 400

```
{  
  "description": "Employee not found by userGuid =  
6ba369e4-b871-4176-8073-a7aaecb6d9d8 and companyId = 2",  
  "code": "NOPAPERPROFILEUL.01005"  
}
```

3.3. Получить информацию о подписях сотрудника

Вызов: **GET** запрос в nopaper

Формат: **JSON**

/partner-api/api/v2/external/certificate/list

1. Авторизация

API-key

2. Входные параметры

Параметр	Обязательность	Тип	Описание	Расположение параметра
userGuid	Да	string	Идентификатор пользователя	Query

Пример запроса

```
https://nopaper-qa.abanking.ru/partner-api/api/v2/external/certificate/list?userGuid=a3b4ea44-bc7a-4c54-ad9e-ba89b1d8f685
```

3. Выходные параметры

В синхронном режиме сервис вернёт статус выполнения запроса.

Code	Description
200	Success
400	Error
401	Unauthorized
403	Forbidden

В случае успешного запроса сервис возвращает массив **certificateInfoList** с информацией о сертификатах пользователя.

Параметр	Тип	Описание
certificateId	integer(\$int32)	Идентификатор сертификата
status	integer(\$int32) / Enum	Статус сертификата
issuedDateTimeUtc	string(\$date-time)	Дата начала действия сертификата
validUntilDateTimeUtc	string(\$date-time)	Дата окончания действия сертификата
ownerName	string	Имя владельца сертификата
ownerGuid	string	Идентификатор владельца сертификата
customData	object	Кастомная информация информация о сертификате

Описание объекта **customData**

PCUserId	string	Идентификатор пользователя РС
SystemId	string	Идентификатор в системе
PublicKey	string	Текст открытого ключа
IssuingType	integer(\$int32) / Enum	Тип выдачи сертификата 1 – Ekys 2 – External

ProviderType	integer(\$int32) / Enum	Криптопровайдер сертификата 1 – PayControl 3 – PayControlServer 5 – CryptoToken 6 – MyDssltm
--------------	-------------------------	--

Пример ответа 200

```
{
  "certificatePCServerInfoList": [
    {
      "certificateId": "1436b2f8-ada3-4384-a042-3d770503bc76",
      "status": 4,
      "issuedDateTimeUtc": "2022-11-30T13:57:38.56048Z",
      "validUntilDateTimeUtc": "2023-11-30T13:57:55Z",
      "ownerName": "Кактус Иван Дмитриевич",
      "ownerGuid": "66310646-97c7-414d-86de-4a9b6023bd5b",
      "customData": {
        "PCUserId":
"ab-PayControlIntegrationApi-0461a76b-83f8-4b47-976d-a4321da46b89",
        "SystemId": "9d8a5fff-5d54-4dfd-918b-3da502bf73aa",
        "PublicKey":
"3059301306072a8648ce3d020106082a8648ce3d03010703420004edeb63bee833d940decce8a1
b333f7b15549d6abb0b12562eb61be29c470955462823c87e363e1c4f0da8f2ec5102108db4fa29
11d0f31eeadaf67815e29fc52",
        "IssuingType": 2,
        "ProviderType": 3
      }
    },
    {
      "certificateId": "e69449c7-8fed-4b83-970b-b5743f8d27aa",
      "status": 2,
      "issuedDateTimeUtc": "2022-12-13T10:46:42.096547Z",
```

```
{
  "validUntilDateTimeUtc": "2023-12-13T10:46:40Z",
  "ownerName": "Кактус Иван Дмитриевич",
  "ownerGuid": "66310646-97c7-414d-86de-4a9b6023bd5b",
  "customData": {
    "PCUserId":
      "ab-PayControlIntegrationApi-21063f2d-6e85-43e9-bc9b-77f790f13c28",
    "SystemId": "9d8a5fff-5d54-4dfd-918b-3da502bf73aa",
    "PublicKey":
      "3059301306072a8648ce3d020106082a8648ce3d030107034200040b5f0300beeeb57b5d4d1cbd
      1f72ccbcc4c0c03ac35462aed0eed08e50adbe4151e292b4d6c7473887821a168a42fcb514f7242
      65dac8887704725c865833de7",
    "IssuingType": 2,
    "ProviderType": 3
  }
}
```

4. Таблица кодов ошибок

—

3.4. Получить акт признания ключа для сертификата

Вызов: **GET** запрос

Формат: **JSON**

/partner-api/api/v2/external/certificate/pay-control/{certificateId}/act-acceptance-key

1. Авторизация

Api-key

2. Входные параметры

Передается в Query

Параметр	Тип	Тип	Описание
certificateId	string(\$uuid)	string(\$uuid)	Идентификатор сертификата

Пример запроса

```
https://nopaper-qa.abanking.ru/partner-api/api/v2/external/certificate/act-acceptance-key?certificateId=5219f2ac-a86f-494b-b5ec-4cbc68aee068
```

3. Выходные параметры

В синхронном режиме сервис вернёт статус выполнения запроса.

Code	Description
200	Success
400	Error
401	Unauthorized

В случае успешного запроса сервис вернёт параметры:

Параметр	Тип	Описание
fileBase64	string	Файл акта признания ключа в формате base64
fileNameWithExtension	string	Название файла с расширением

4. Таблица кодов ошибок

Код	Текст	Комментарий
PAYCONTROLINTEGRATIONAPI.00214	Keys must be installed	Для сертификата ещё не сформирован публичный ключ подписи – сертификат не завершил инициализацию

Пример ответа с кодом 400

```
{
  "description": "Keys must be installed",
  "code": "PAYCONTROLINTEGRATIONAPI.00214"
}
```

3.5. Активировать подпись сотрудника

Вызов: **PATCH** запрос в порарер

Формат: **JSON**

/partner-api/api/v2/external/certificate/pay-control/{certificateId}/activate

1. Авторизация

API-key

2. Входные параметры

[postman collection](#) (версия 1.0)

Параметр	Тип	Обязательность	Описание	Расположение параметра
certificateId	string(\$uuid)	Да	Идентификатор сертификата	Route

Пример запроса

```
{{demo}}/partner-api/api/v2/external/certificate/pay-control/f6af18b9-7ecb-4a59-a473-0d44f232cf35/activate
```

3.В синхронном режиме сервис вернёт статус выполнения запроса.

Code	Description
200	Success
400	Error
401	Unauthorized
403	Forbidden

В случае успешного запроса сервис вернёт 200 OK.

4. Таблица кодов ошибок

Код	Текст	Комментарий
NOPAPERPARTNER.10352	Unable to change status from Available to Available	Сертификат уже активирован

[postman collection](#) (версия 1.0)

SIGNINGAPI.CORE.04008	CertificateDal not found by key= {certificateId}	Сертификат отсутствует в сервисе
NOPAPERPARTNER.10350	client-api not have link with certificate	Сертификат не создан данным Партнером
NOPAPERPARTNER.10352	Unable to change status from Template to Available	Невозможно активировать сертификат из текущего статуса
PAYCONTROL.00003	Key acceptance act must be generated before accepting	Необходимо принять акт признания ключа перед активацией

Пример ответа с кодом 400

```
{
  "description": "Unable to change status from Available to Available",
  "code": "NOPAPERPARTNER.10352"
}
```

3.6. Заблокировать/активировать подпись

Вызов: **PATCH** запрос в nopaper**Формат:** **JSON****`/partner-api/api/v2/external/certificate/pay-control/{certificateId}/blocking-control`**

1. Авторизация

API-key

2. Входные параметры

Параметр	Тип	Обязательность	Описание	Расположение параметра
certificatelid	string (\$uuid)	Да	Идентификатор сертификата	Route
isBlock	bool	Да	true = заблокировать сертификат false = разблокировать сертификат	Query

Пример запроса

```
/partner-api/api/v2/external/certificate/pay-control/615f4f65-d42a-4144-a3b7-f69e5ea8aed6/blocking-control?isBlock=false
```

3. Выходные параметры

В синхронном режиме сервис вернёт статус выполнения запроса.

Code	Description
200	Success
400	Error

401	Unauthorized
403	Forbidden

В случае успешного запроса сервис вернёт 200 OK.

4. Таблица кодов ошибок

Код	Текст	Комментарий
NOPAPERPARTNER.10352	Unable to change status from Available to Available Unable to change status from Blocked to Blocked	Сертификат в состоянии разблокирован/заблокирован
SIGNINGAPI.CORE.04008	CertificateDal not found by key={certificateId}	Сертификат отсутствует в сервисе
NOPAPERPARTNER.10350	client-api not have link with certificate	Сертификат не создан данным Партнёром

Пример ответа с кодом 400

```
{  
  "description": "Unable to change status from Blocked to Blocked",  
  "code": "NOPAPERPARTNER.10352"  
}
```

3.7. Отозвать подпись сотрудника

Вызов: **PATCH** запрос в порарер

Формат: **JSON**

/partner-api/api/v2/external/certificate/pay-control/{certificateId}/revoke

1. Авторизация

API-key

2. Входные параметры

Параметр	Тип	Обязательность	Описание	Расположение параметра
certificateId	string(\$uuid)	Да	Идентификатор сертификата	Route

Пример запроса

```
/partner-api/api/v2/external/certificate/pay-control/f6af18b9-7ecb-4a59-a473-0d44f232cf35/revoke
```

3. Выходные параметры

В синхронном режиме сервис вернёт статус выполнения запроса.

Code	Description
------	-------------

200	Success
400	Error
401	Unauthorized
403	Forbidden

В случае успешного запроса сервис вернёт 200 OK.

4. Таблица кодов ошибок

Код	Текст	Комментарий
SIGNING.00014	Wrong next certificate-provider status Revoked for current Revoked	Сертификат уже в состоянии отозван
SIGNINGAPI.CORE.04008	CertificateDal not found by key= {certificateId}	Сертификат отсутствует в сервисе
NOPAPERPARTNER.10350	client-api not have link with certificate	Сертификат не создан данным Партнёром

Пример ответа с кодом 400

```
{
  "description": "Wrong next certificate-provider status Revoked for current Revoked",
  "code": "SIGNING.00014"
}
```